DHR
Administrative Services
Privacy Act of 1974
PII Training

May 2013

Definition

- The **Privacy Act of 1974** (Pub.L.93-579, 88 Stat. 1896, enacted December 31, 1974, 5 U.S.C. Section 552a) establishes a Code of Fair Information Practice that governs the collection, maintenance, use, and dissemination of **personally identifiable information (PII)** about individuals that is maintained in systems of records by federal agencies.

Basic Policy Objectives

- To **restrict disclosure of personally identifiable** records maintained by Executive branch agencies.
- To grant individuals increased **rights of access to** agency records maintained on themselves.
- To grant individuals the **right to seek amendment of** agency records that are not accurate, relevant, timely, or complete.
- To establish a **code of "fair information practices”** which regulates the collection, use, maintenance and disclosure of personally identifiable information

Privacy Act Pertains To

Privacy Act protects information on individuals that is in a "**system of records**"

- This is any group of records from which information is **retrieved by the name of an individual or by some** other identifying particular assigned to the individual.
  - Must identify the individual.
  - Must be retrieved by an identifier.
- Excludes
  - purely personal notes
  - supervisory notes (memory refreshers)

Disclosure

General Rule - NO disclosure unless you have:

- Individual is requesting in person.
- Written request from the subject.
- Prior written consent from the subject authorizing a 3rd party to gain access.

Privacy Act Violation

- You have violated the Privacy Act if you have either knowingly or unknowingly released/disclosed individual PII to a third party without the knowledge and approval of the individual.
- This would include any **combination of Name** with the individuals:
  - **SSN**
  - **Phone Number**
  - **Email Address**
  - **Physical Address**
  - **Official Titles**

Violations Are Illegal

Misdemeanor and fine not to exceed $5,000

- Any officer, NCO, or employee who knowingly and willingly discloses identifiable information to any person who is not entitled to receive it.
- Any officer, NCO, or employee who willfully maintains a “secret” system of records.
- Knowingly and willingly requests or obtains Privacy Act protected records under false pretenses.

Safeguarding PII

- PII must be processed following the procedures used to process and access information designated “FOUO.”
- PII must be protected while it is being processed or accessed in computer environments.
  - Use a **Data at Rest (DAR)** folder on your desktop. NEC JBLM PII SOP explains how to setup DAR folder.
  - When emailing outside of a government system encrypt email; or use the **AMRDEC Safe Access File Exchange (SAFE)**. Handout Provided

Exception to Encryption

The following guidance from the Army Privacy Office addresses PII on government computers. Emailing PII unencrypted on a system **.mil to .gov, .gov to .gov, or .mil to .mil etc. communication with a need to know is not considered a PII compromise.** There is an expectation of security within the government's computer network system. All government systems abide by standards set by the National Institute of Standards and Technology (NIST). One of NIST's missions is to promote standards, for government Information Technology that enhances security